Session on the

Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence

Alexander Seger
Executive Secretary Cybercrime Convention Committee (T-CY)
Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

The mechanism of the Budapest Convention

Budapest Convention on Cybercrime (2001):

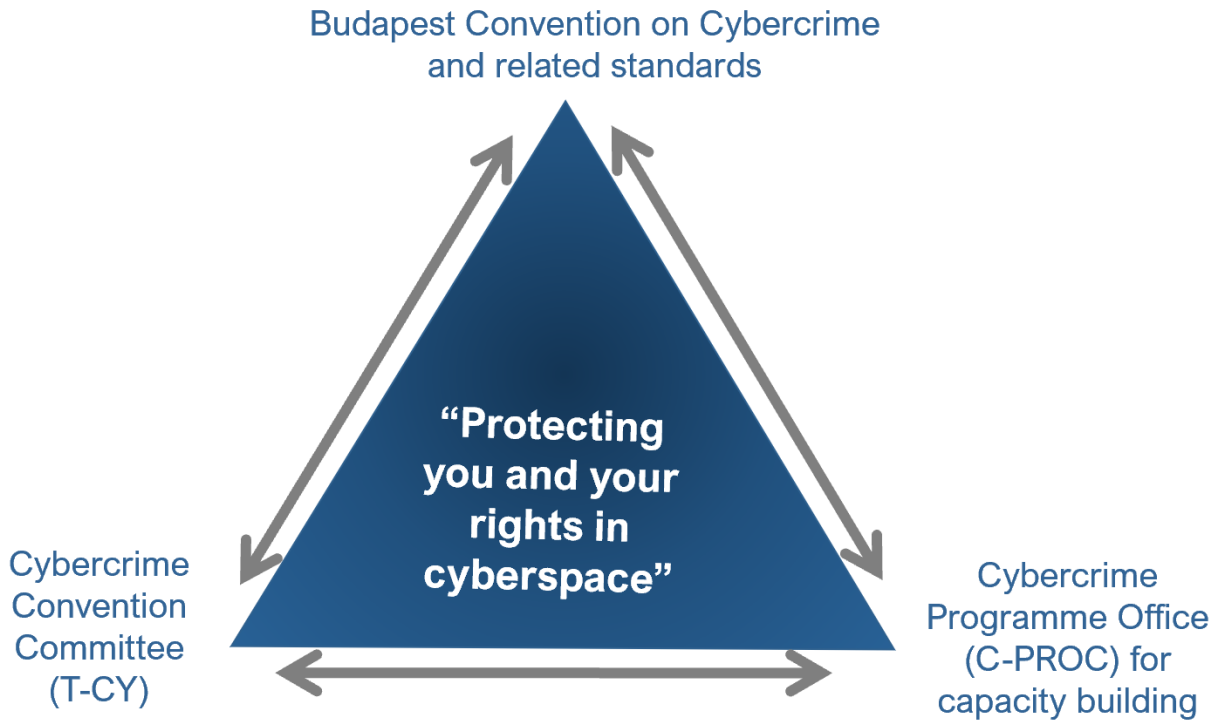
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

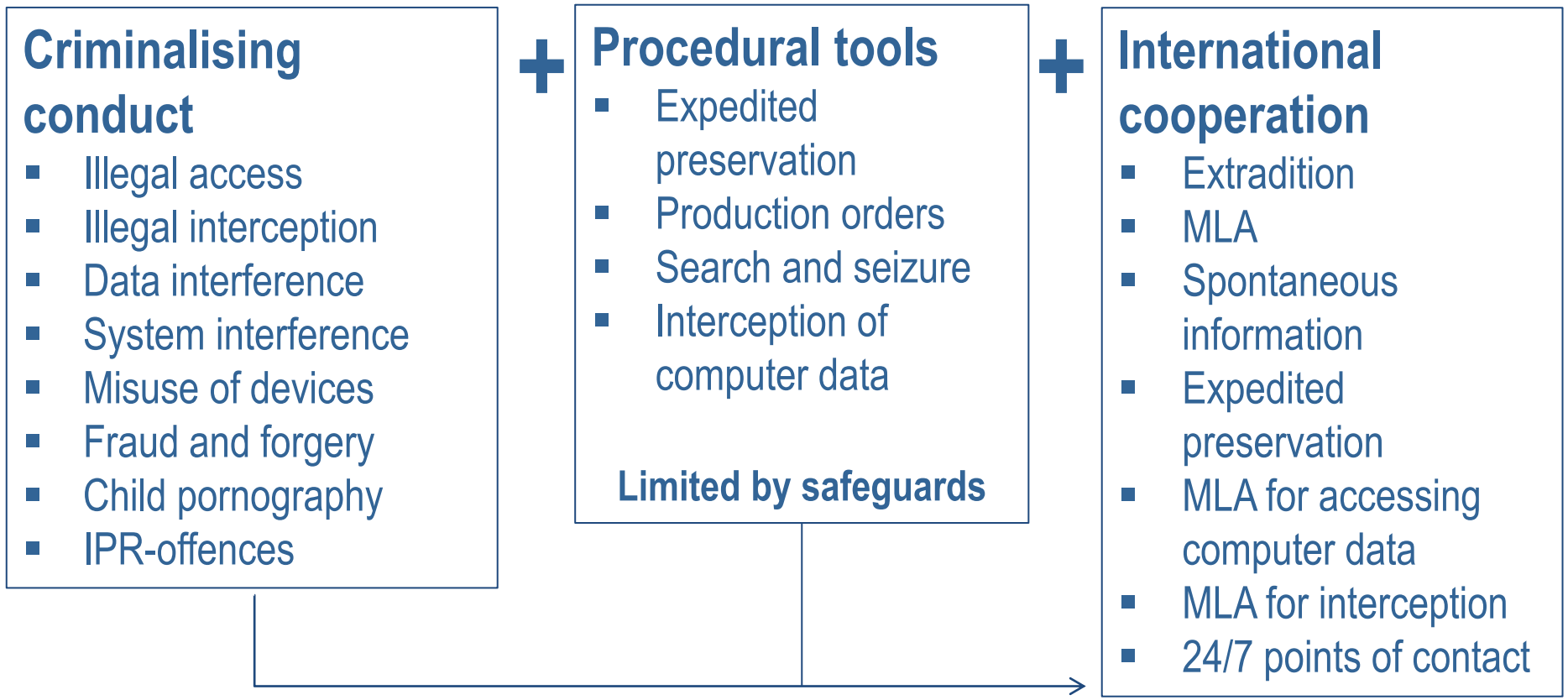
+ Guidance Notes

+ Protocol on enhanced cooperation on cybercrime and electronic evidence in preparation

By June 2021: 66 Parties and 11 Observer States



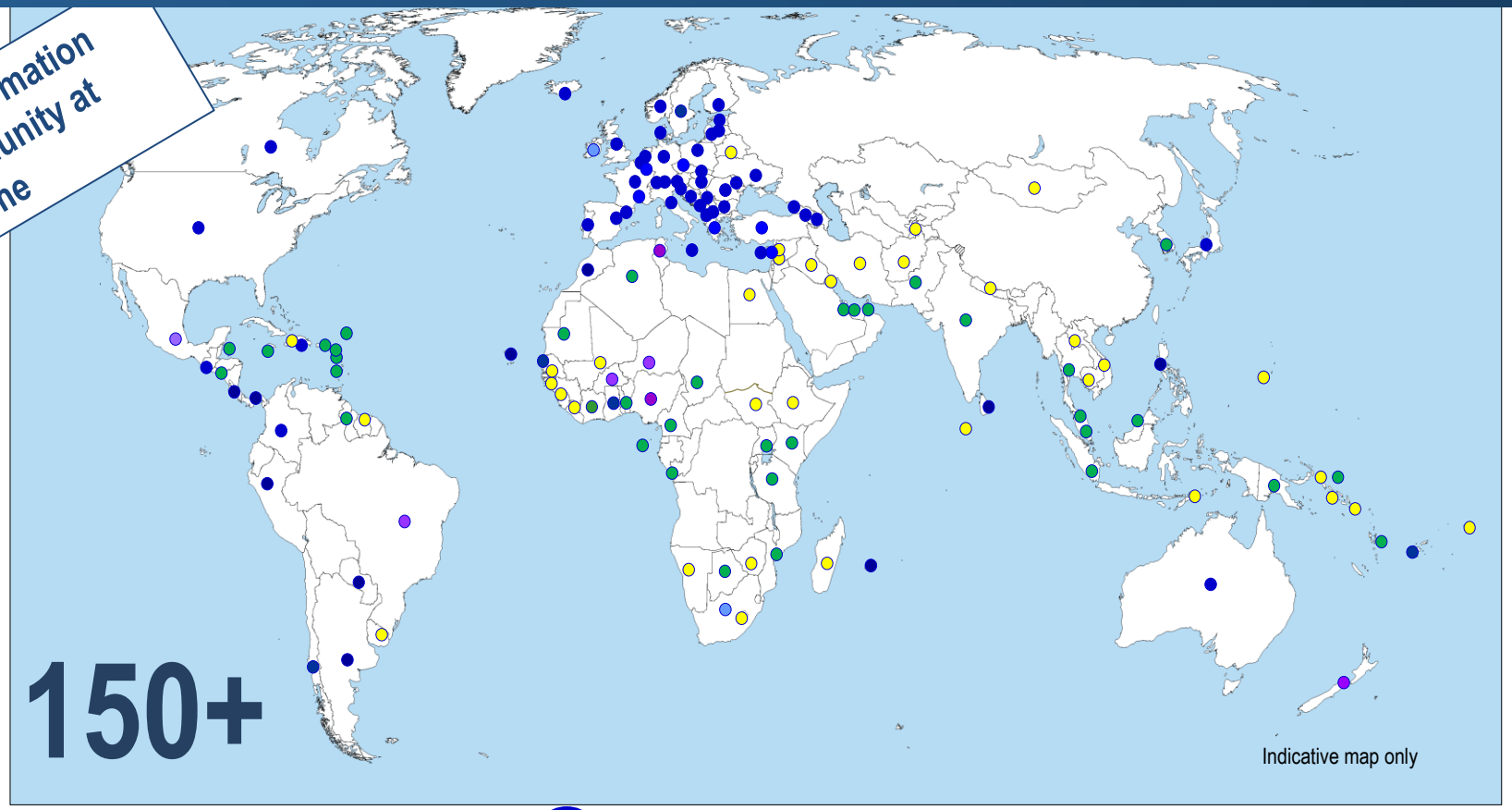
Content of the Budapest Convention



Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!

Reach of the Budapest Convention

For country-specific information see the Octopus Community at www.coe.int/cybercrime



Parties:	66
Signed:	2
Invited to accede:	9
=	77

Other States with laws largely in line with Budapest Convention = 20+

Further States drawing on Budapest Convention for legislation = 50+

Africa and Budapest Convention

Parties:
- Cabo Verde
- Ghana
- Mauritius
- Morocco
- Senegal

Signatory:
- South Africa

Invited to accede:
- Benin
- Burkina Faso
- Niger
- Nigeria
- Tunisia

Rationale: Why a 2nd Additional Protocol to the Budapest Convention?

- The scale and quantity of cybercrime, devices, users and victims
- Cloud computing, territoriality and jurisdiction
  - Where is the crime?
  - Where is the data, where is the evidence?
  - Who has the evidence?
  - What legal regime applies to order / disclose data?
- The challenge of mutual legal assistance
- The "<1% problem"

- How to obtain subscriber information efficiently?
- How to cooperate directly with a service provider in another Party?
- How to obtain WHOIS data (domain name registration information) from registrars?
- How to obtain stored data, including content, in an emergency situation?
- How to make mutual assistance more effective?
- How to reconcile efficient and effective measures with rule of law and data protection requirements?

Background to the 2nd Additional Protocol to the Budapest Convention on Cybercrime

- Preparatory work of the Cybercrime Convention Committee (T-CY):
  - Transborder Group (2012-2014)
  - Assessment of MLA provisions (2014)
  - Cloud Evidence Group (2014- 2017)
  - Need for Protocol identified

- June 2017: Terms of reference for preparation of the Protocol adopted by the T-CY
- September 2017 – May 2021:
  - 10 Drafting Plenaries + 16 Drafting Group meeting + 65 virtual subgroup meetings + 6 rounds of consultations + numerous bi/trilateral meetings + domestic meetings
- 28 May 2021: Draft Protocol approved by T-CY

Next:

- Formal adoption (November 2021 TBC)
- Opening for signature (March 2022 TBC)

2nd Additional Protocol to the Convention on Cybercrime: content

Preamble

Chapter I: Common provisions

Article 1 Purpose
Article 2 Scope of application
Article 3 Definitions
Article 4 Language

Chapter II: Measures for enhanced cooperation

Article 5 General principles applicable to Chapter II
Article 6 Request for domain name registration information
Article 7 Disclosure of subscriber information
Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data
Article 9 Expedited disclosure of stored computer data in an emergency
Article 10 Emergency mutual assistance
Article 11 Video conferencing
Article 12 Joint investigation teams and joint investigations

Chapter III – Conditions and safeguards

Article 13 Conditions and safeguards
Article 14 Protection of personal data

Chapter IV: Final provisions

Article 15 Effects of this Protocol
Article 16 Signature and entry into force
Article 17 Federal clause
Article 18 Territorial application
Article 19 Reservations and declarations
Article 20 Status and withdrawal of reservations
Article 21 Amendments
Article 22 Settlement of disputes
Article 23 Consultations of the Parties and assessment of implementation
Article 24 Denunciation
Article 25 Notification

Benefits of the Protocol

Operational value:

- Basis for direct cooperation with service providers for subscriber information ("direct disclosure")
- Effective means to obtain subscriber information and traffic data ("giving effect")
- Legal basis for disclosure of WHOIS information
- Cooperation in emergencies ("expedited disclosure" + "emergency MLA")
- Mutual assistance tools ("video-conferencing", "JITs")
- Data protection safeguards to permit the flow of personal data under the Protocol

Policy value:

- Convention on Cybercrime will remain relevant and effective
- Efficient cooperation with rule of law and data protection safeguards is feasible
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)